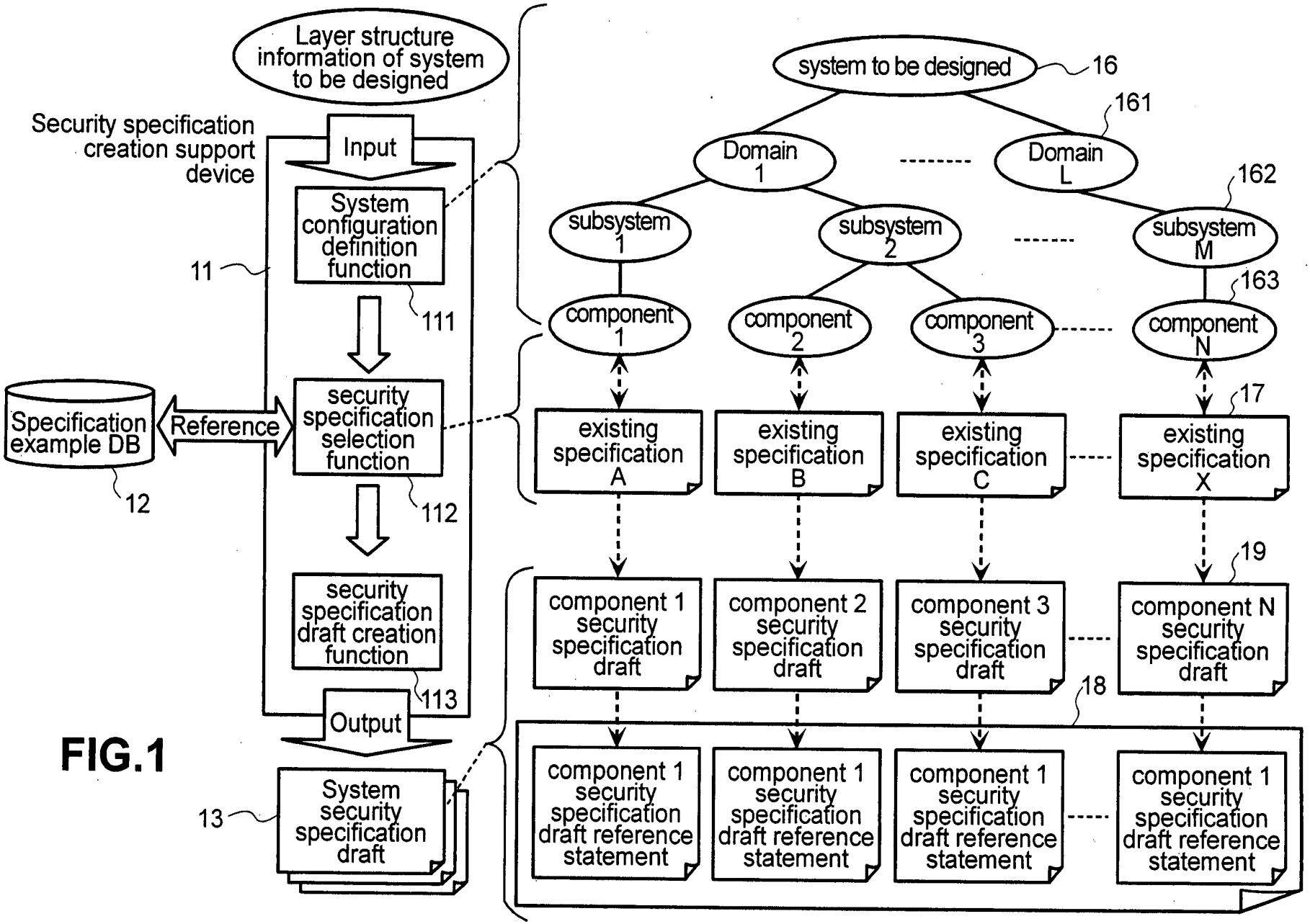

Layer structure information of system to be designed
Security specification creation support device
Input
System configuration definition function
11
111
security specification selection function
Specification example DB
Reference
12
112
security specification draft creation function
113
Output
System security specification draft
13
system to be designed
16
161
Domain 1
Domain L
162
subsystem 1
subsystem 2
subsystem M
163
component 1
component 2
component 3
component N
17
existing specification A
existing specification B
existing specification C
existing specification X
19
component 1 security specification draft
component 2 security specification draft
component 3 security specification draft
component N security specification draft
18
component 1 security specification draft reference statement
component 1 security specification draft reference statement
component 1 security specification draft reference statement
component 1 security specification draft reference statement

FIG.1

FIG.2

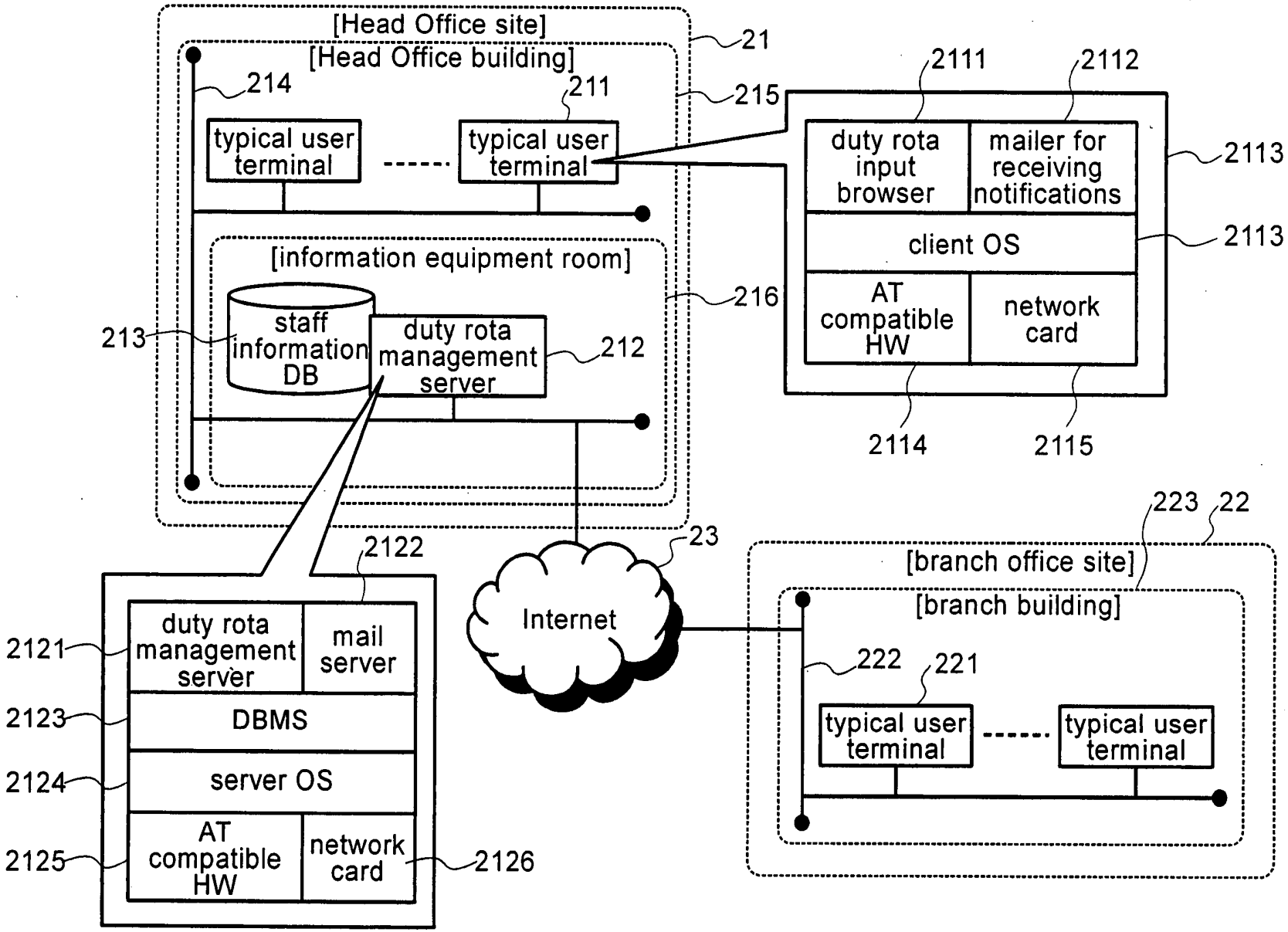

[Head Office site]
21
[Head Office building]
214
211
215
typical user terminal
typical user terminal
2111
2112
duty rota input browser
mailer for receiving notifications
2113
client OS
2113
AT compatible HW
network card
2114
2115
[information equipment room]
216
213
staff information DB
duty rota management server
212
223
22
[branch office site]
[branch building]
222
221
typical user terminal
typical user terminal
23
Internet
2122
2121
duty rota management server
mail server
2123
DBMS
2124
server OS
2125
AT compatible HW
network card
2126

FIG.3

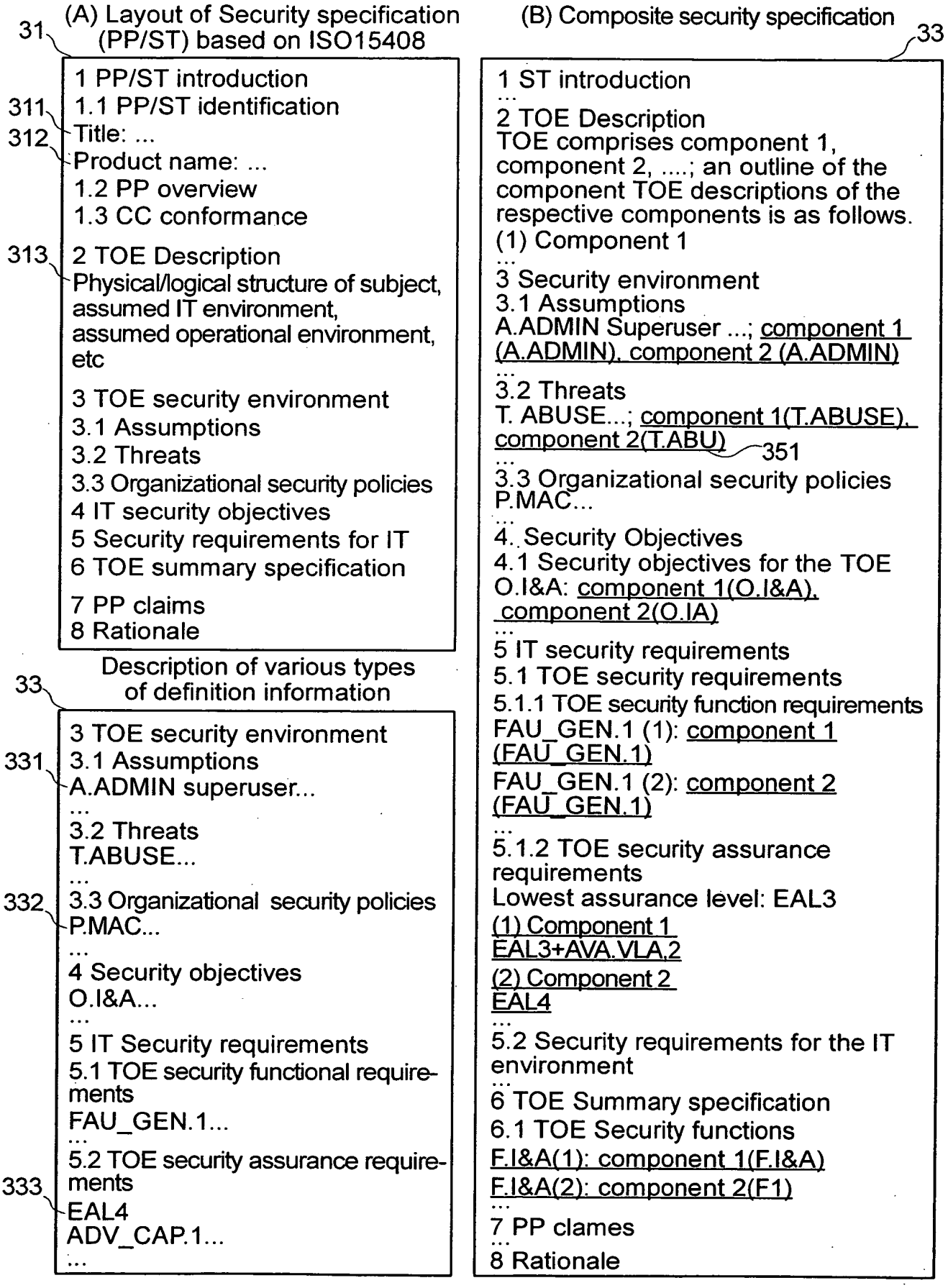

(A) Layout of Security specification (PP/ST) based on ISO15408
31
1 PP/ST introduction
311
1.1 PP/ST identification
312
Title: ...
Product name: ...
1.2 PP overview
1.3 CC conformance
313
2 TOE Description
Physical/logical structure of subject, assumed IT environment, assumed operational environment, etc
3 TOE security environment
3.1 Assumptions
3.2 Threats
3.3 Organizational security policies
4 IT security objectives
5 Security requirements for IT
6 TOE summary specification
7 PP claims
8 Rationale
Description of various types of definition information
33
3 TOE security environment
331
3.1 Assumptions
A.ADMIN superuser...
...
3.2 Threats
T.ABUSE...
...
332
3.3 Organizational security policies
P.MAC...
...
4 Security objectives
O.I&A...
...
5 IT Security requirements
5.1 TOE security functional requirements
FAU_GEN.1...
...
5.2 TOE security assurance requirements
333
EAL4
ADV_CAP.1...
...
(B) Composite security specification
33
1 ST introduction
...
2 TOE Description
TOE comprises component 1, component 2, ...; an outline of the component TOE descriptions of the respective components is as follows.
(1) Component 1
...
3 Security environment
3.1 Assumptions
A.ADMIN Superuser ...; component 1 (A.ADMIN), component 2 (A.ADMIN)
...
3.2 Threats
T. ABUSE...; component 1(T.ABUSE), component 2(T.ABU)
351
...
3.3 Organizational security policies
P.MAC...
...
4. Security Objectives
4.1 Security objectives for the TOE
O.I&A: component 1(O.I&A), component 2(O.IA)
...
5 IT security requirements
5.1 TOE security requirements
5.1.1 TOE security function requirements
FAU_GEN.1 (1): component 1 (FAU_GEN.1)
FAU_GEN.1 (2): component 2 (FAU_GEN.1)
...
5.1.2 TOE security assurance requirements
Lowest assurance level: EAL3
(1) Component 1
EAL3+AVA.VLA.2
(2) Component 2
EAL4
...
5.2 Security requirements for the IT environment
...
6 TOE Summary specification
6.1 TOE Security functions
F.I&A(1): component 1(F.I&A)
F.I&A(2): component 2(F1)
...
7 PP clames
...
8 Rationale

FIG.4

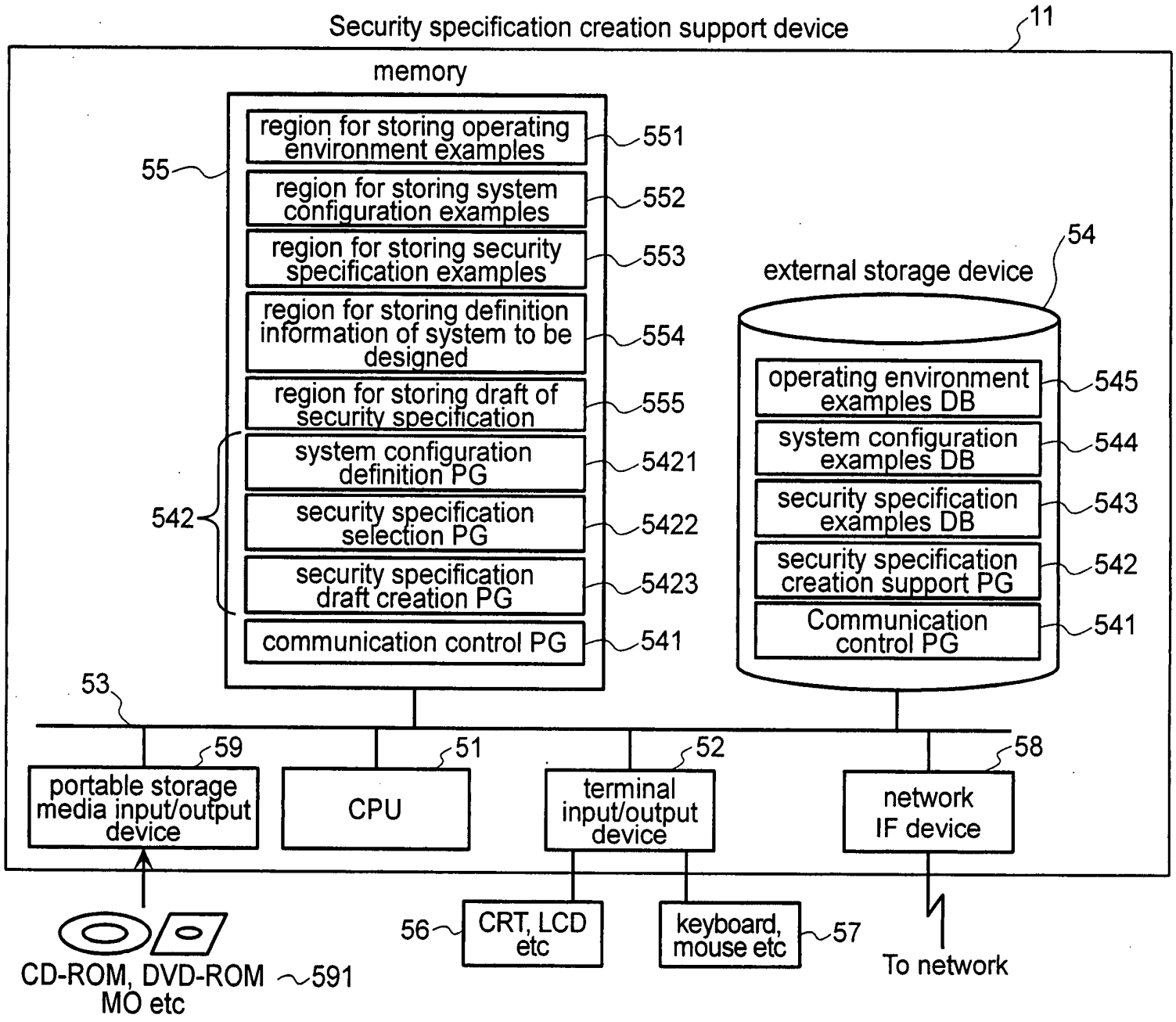

Security specification creation support device
11
memory
55
region for storing operating environment examples
551
region for storing system configuration examples
552
region for storing security specification examples
553
region for storing definition information of system to be designed
554
region for storing draft of security specification
555
542
system configuration definition PG
5421
security specification selection PG
5422
security specification draft creation PG
5423
communication control PG
541
54
external storage device
operating environment examples DB
545
system configuration examples DB
544
security specification examples DB
543
security specification creation support PG
542
Communication control PG
541
53
59
portable storage media input/output device
51
CPU
52
terminal input/output device
58
network IF device
CD-ROM, DVD-ROM MO etc
591
56
CRT, LCD etc
keyboard, mouse etc
57
To network

FIG.5

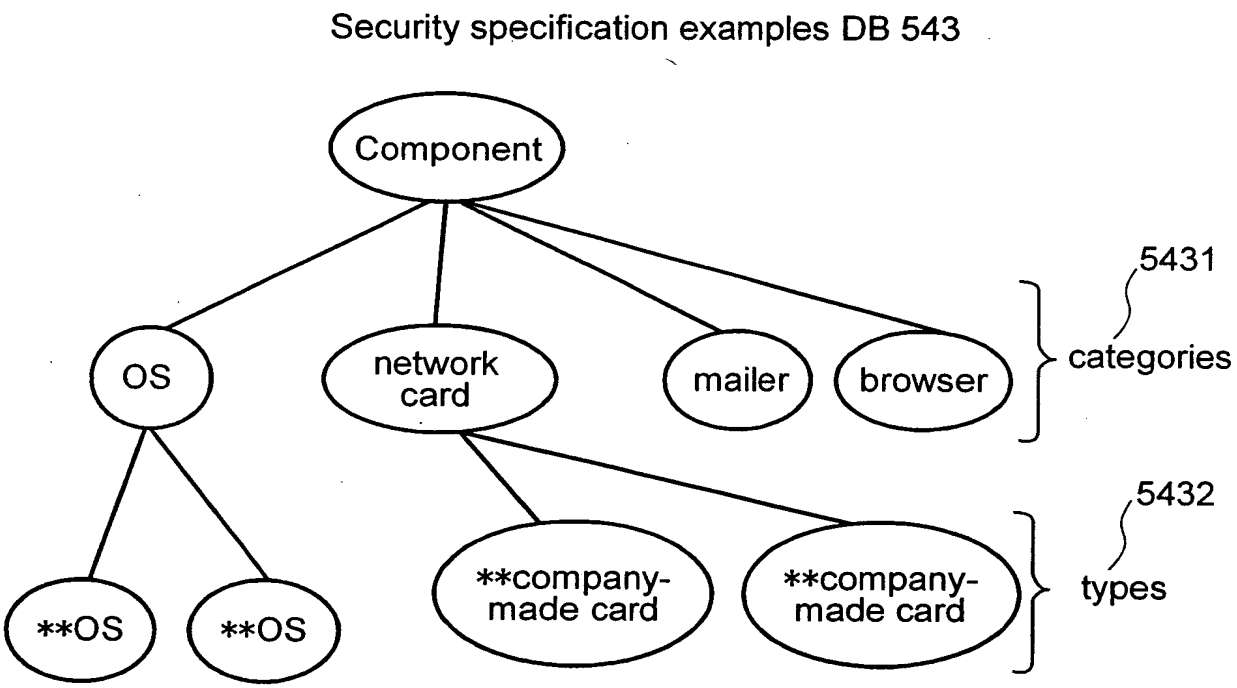

Security specification examples DB 543
Component
OS
network card
mailer
browser
5431
categories
**OS
**OS
**company-made card
**company-made card
5432
types

FIG.6

System configuration examples DB544

< subsystem > 5443a
< element name > IT equipment < /element name > 5446
< component >
< element name > application layer < /element name >
< /component >
< component > 5444a
< element name > middleware layer < /element name > 5447
< /component >
< component > 5444b
< element name > OS layer < /element name >
< /component >
< component >
< element name > hardware layer < /element name >
< /component >
< /subsystem > 5443b

5441 System deployment pattern

< subsystem >
< element name > IC card < /element name >
< component >
< element name > application layer < /element name >
< /component >
< component >
< element name > OS layer < /element name >
< /component >
< component >
< element name > hardware layer < /element name >
< /component >
< /subsystem >

< subsystem >
< element name > H Inc IC card < /element name >
< component >
< element name > application < /element name >
< definition text > < /definition text >
< specification > < /specification >
< /component >
< component >
< element name > IC card OS < /element name >
< definition text > This IC card OS... < /definition text >
< specification > "A Inc IC card OS ST v2.0" < /specification>
< /component >
< component >
< element name > IC chip < /element name >
< definition text > This IC chip... < /definition text >
< specification > "H Inc IC chip ST v1.1" < /specification >
< /component >
< /subsystem >

FIG.7

Operational environment example DB545

< subsystem >
< element name > IT equipment < /element name >
< operation > Operation is performed to ensure password secrecy < /operation >
< component >
< element name > application layer < /element name >
< operation > The password is not displayed on the screen when input. < /operation >
< operation > The password is not recorded in a readable form on paper or the like. < /operation >
...
< /component >
< component >
< element name > OS layer < /element name >
< operation > The password is not displayed on the screen when input. < /operation >
< operation > The password is not recorded in a readable form on paper or the like. < /operation >
< operation > The password is periodically changed. < /operation >
...
< /component >
< /subsystem >

< subsystem >
...
< /subsystem >

5452

5451
Operational environment pattern

FIG.8

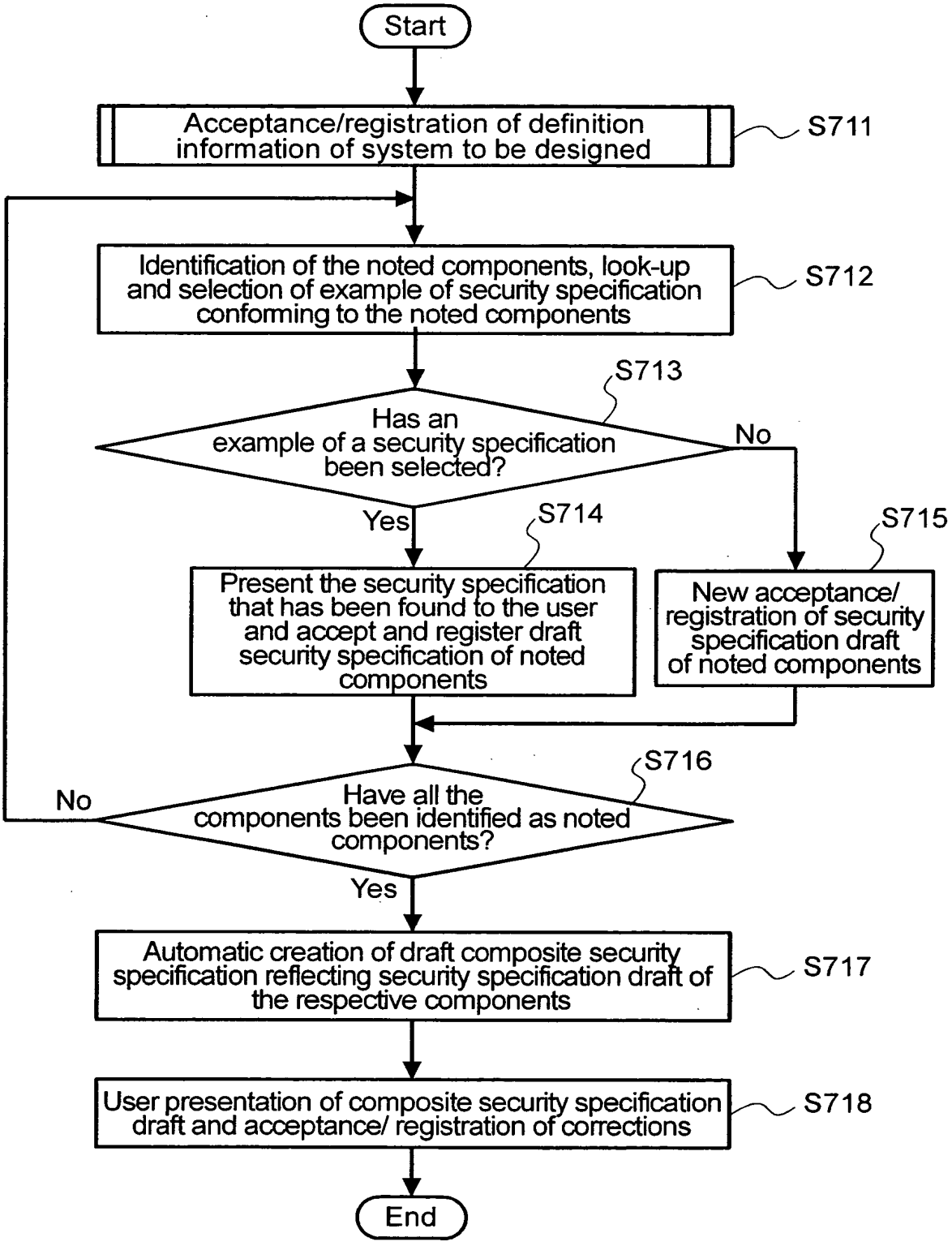

Start
Acceptance/registration of definition information of system to be designed
S711
Identification of the noted components, look-up and selection of example of security specification conforming to the noted components
S712
S713
Has an example of a security specification been selected?
No
Yes
S714
S715
Present the security specification that has been found to the user and accept and register draft security specification of noted components
New acceptance/ registration of security specification draft of noted components
S716
No
Have all the components been identified as noted components?
Yes
Automatic creation of draft composite security specification reflecting security specification draft of the respective components
S717
User presentation of composite security specification draft and acceptance/ registration of corrections
S718
End

FIG.9

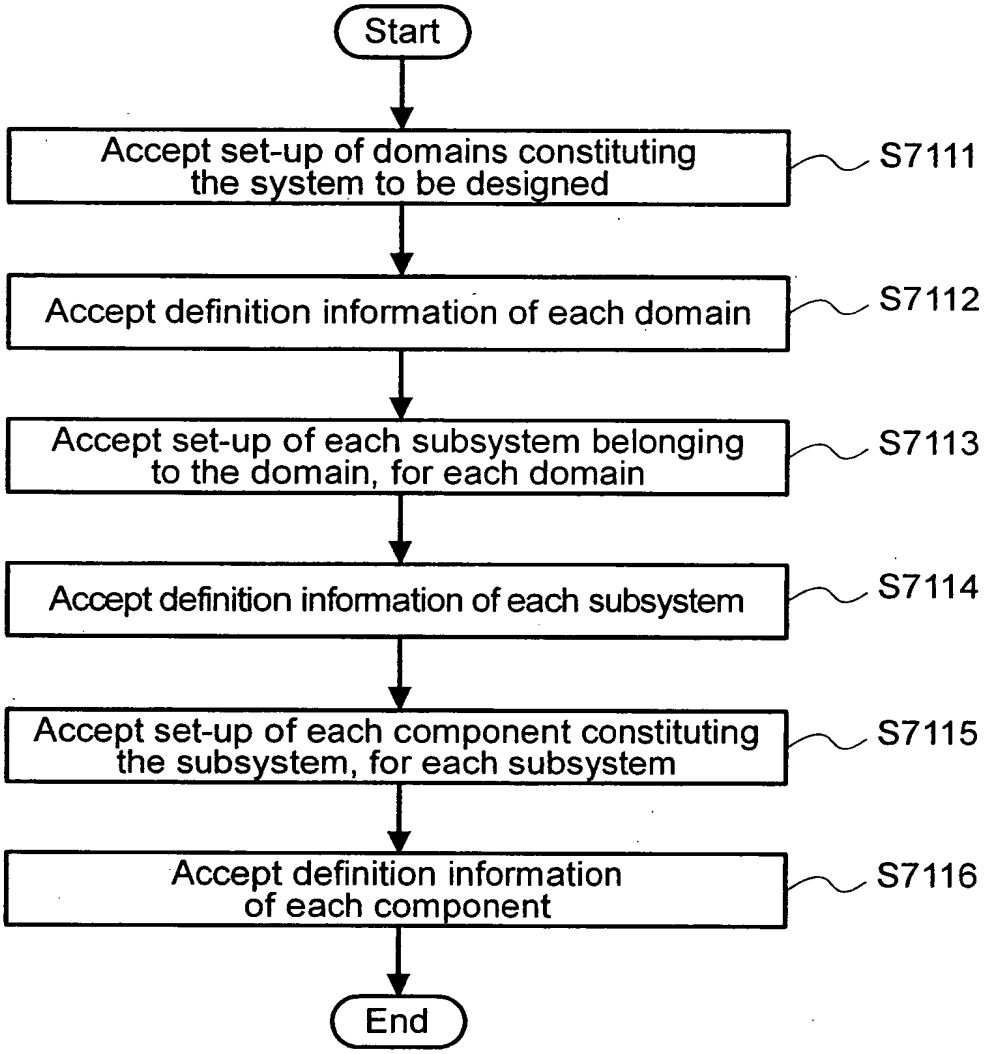

Start
Accept set-up of domains constituting the system to be designed
S7111
Accept definition information of each domain
S7112
Accept set-up of each subsystem belonging to the domain, for each domain
S7113
Accept definition information of each subsystem
S7114
Accept set-up of each component constituting the subsystem, for each subsystem
S7115
Accept definition information of each component
S7116
End

FIG.10

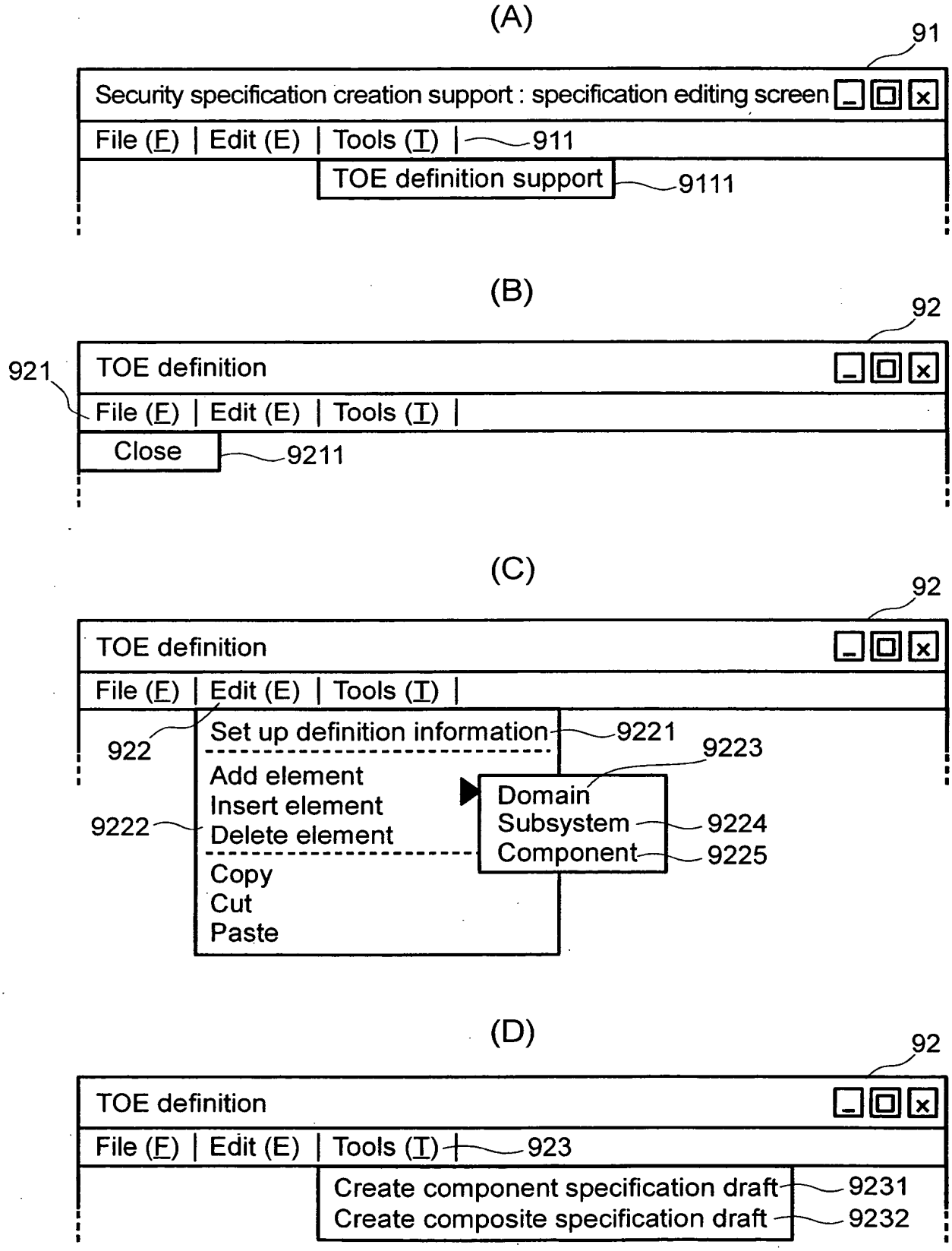

(A)
91
Security specification creation support : specification editing screen
File (F) | Edit (E) | Tools (T) |
911
TOE definition support
9111
(B)
92
921
TOE definition
File (F) | Edit (E) | Tools (T) |
Close
9211
(C)
92
TOE definition
File (F) | Edit (E) | Tools (T) |
922
Set up definition information
9221
9223
Add element
Insert element
Delete element
9222
Copy
Cut
Paste
Domain
Subsystem
9224
Component
9225
(D)
92
TOE definition
File (F) | Edit (E) | Tools (T)
923
Create component specification draft
9231
Create composite specification draft
9232

FIG.11

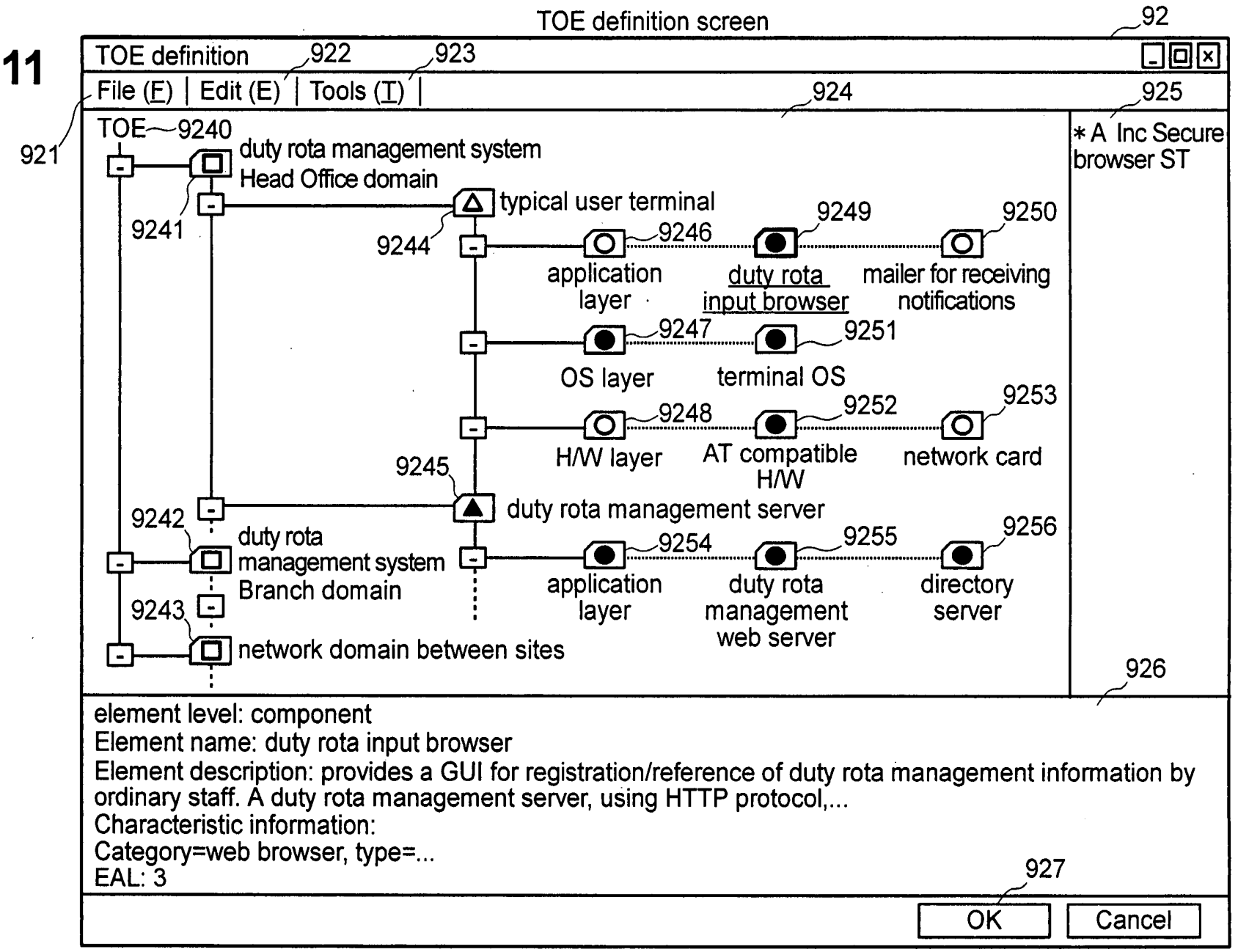

TOE definition screen
92
TOE definition
922
923
File (F) | Edit (E) | Tools (T) |
924
925
921
TOE
9240
duty rota management system
Head Office domain
9241
typical user terminal
9244
9246
9249
9250
application layer
duty rota input browser
mailer for receiving notifications
9247
9251
OS layer
terminal OS
9248
9252
9253
H/W layer
AT compatible H/W
network card
9245
duty rota management server
9242
duty rota management system
Branch domain
9254
9255
9256
application layer
duty rota management web server
directory server
9243
network domain between sites
* A Inc Secure browser ST
926
element level: component
Element name: duty rota input browser
Element description: provides a GUI for registration/reference of duty rota management information by ordinary staff. A duty rota management server, using HTTP protocol,...
Characteristic information:
Category=web browser, type=...
EAL: 3
927
OK
Cancel

FIG.12

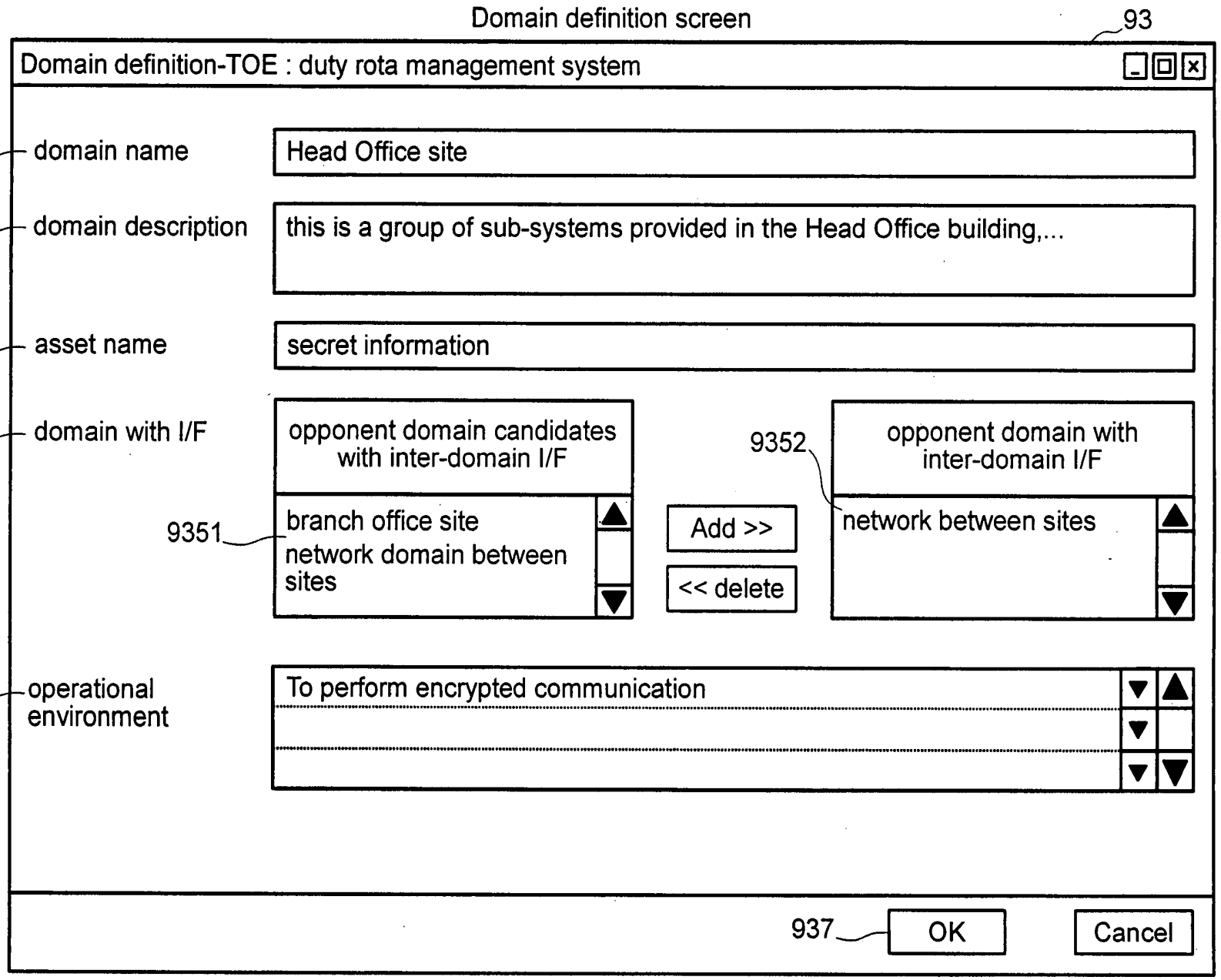

Domain definition screen
93
Domain definition-TOE : duty rota management system
932
domain name
Head Office site
933
domain description
this is a group of sub-systems provided in the Head Office building,...
934
asset name
secret information
935
domain with I/F
opponent domain candidates with inter-domain I/F
9351
branch office site
network domain between sites
Add >>
<< delete
9352
opponent domain with inter-domain I/F
network between sites
936
operational environment
To perform encrypted communication
937
OK
Cancel

FIG.13

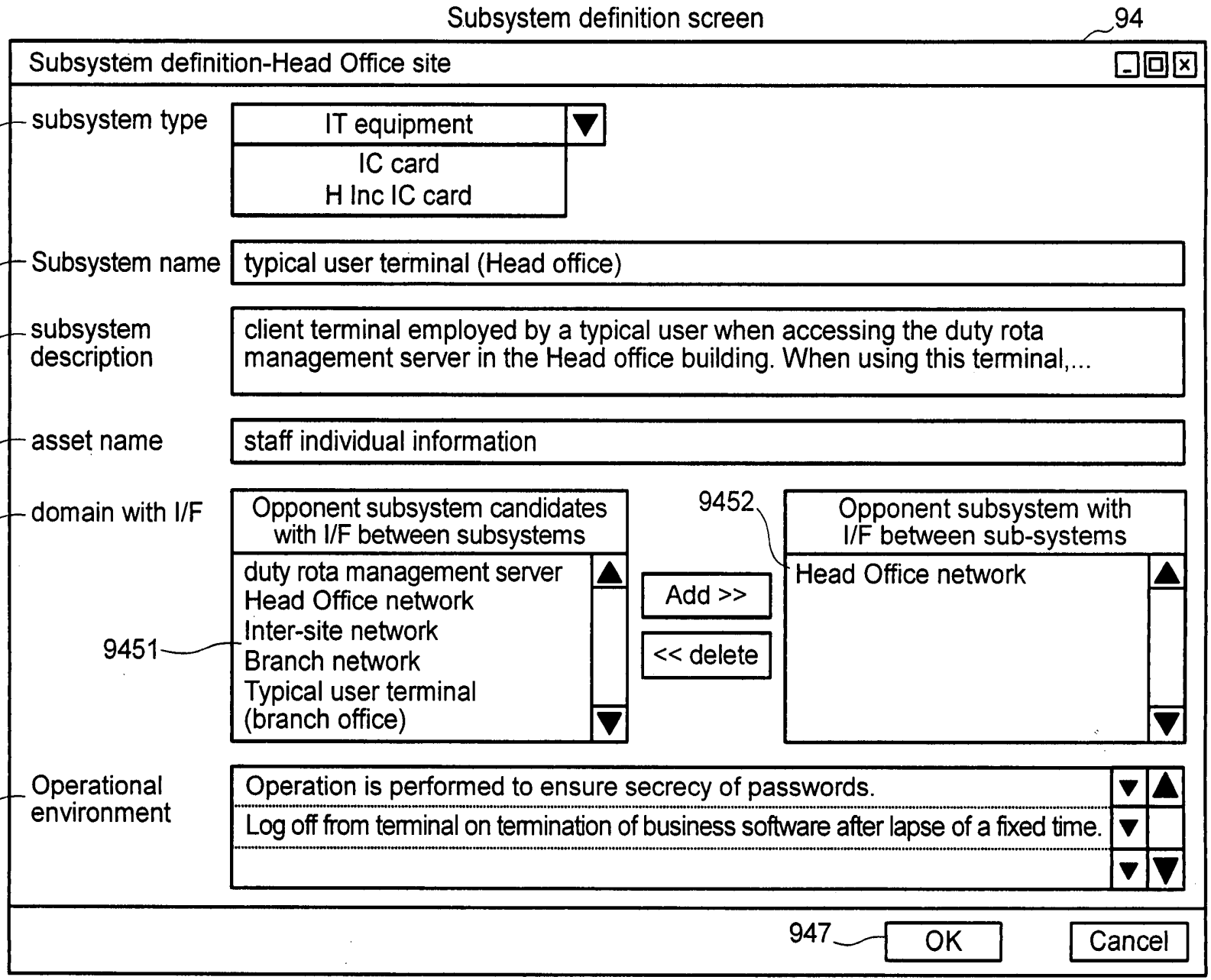

Subsystem definition screen
94
Subsystem definition-Head Office site
941
subsystem type
IT equipment
IC card
H Inc IC card
942
Subsystem name
typical user terminal (Head office)
943
subsystem description
client terminal employed by a typical user when accessing the duty rota management server in the Head office building. When using this terminal,...
944
asset name
staff individual information
945
domain with I/F
Opponent subsystem candidates with I/F between subsystems
duty rota management server
Head Office network
Inter-site network
Branch network
Typical user terminal (branch office)
9451
Add >>
<< delete
9452
Opponent subsystem with I/F between sub-systems
Head Office network
946
Operational environment
Operation is performed to ensure secrecy of passwords.
Log off from terminal on termination of business software after lapse of a fixed time.
947
OK
Cancel

FIG.14

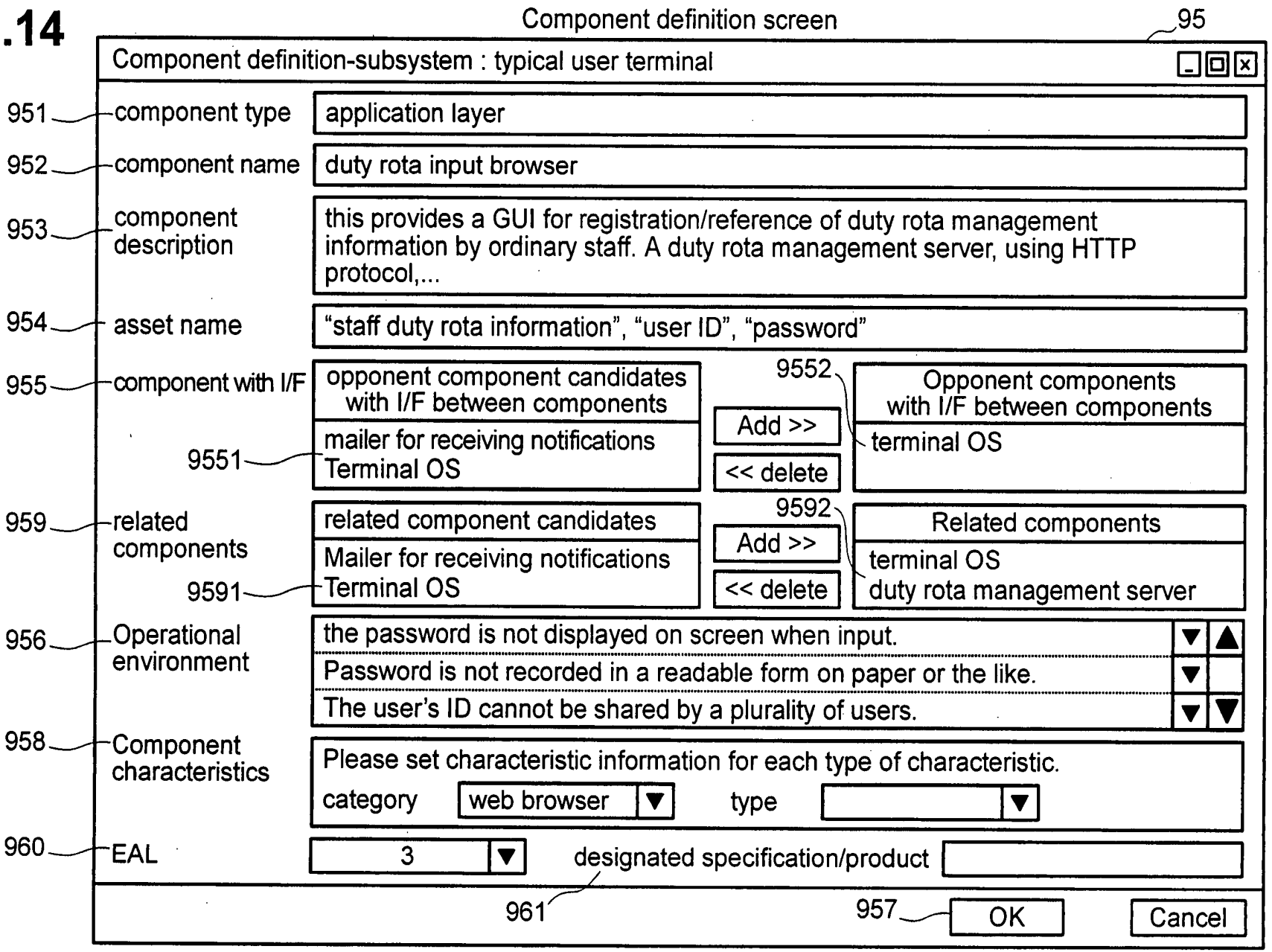

Component definition screen
95
Component definition-subsystem : typical user terminal
951
component type
application layer
952
component name
duty rota input browser
953
component description
this provides a GUI for registration/reference of duty rota management information by ordinary staff. A duty rota management server, using HTTP protocol,...
954
asset name
"staff duty rota information", "user ID", "password"
955
component with I/F
opponent component candidates with I/F between components
mailer for receiving notifications
Terminal OS
9551
Add >>
<< delete
9552
Opponent components with I/F between components
terminal OS
959
related components
related component candidates
Mailer for receiving notifications
Terminal OS
9591
Add >>
<< delete
9592
Related components
terminal OS
duty rota management server
956
Operational environment
the password is not displayed on screen when input.
Password is not recorded in a readable form on paper or the like.
The user's ID cannot be shared by a plurality of users.
958
Component characteristics
Please set characteristic information for each type of characteristic.
category
web browser
type
960
EAL
3
designated specification/product
961
957
OK
Cancel

FIG.15

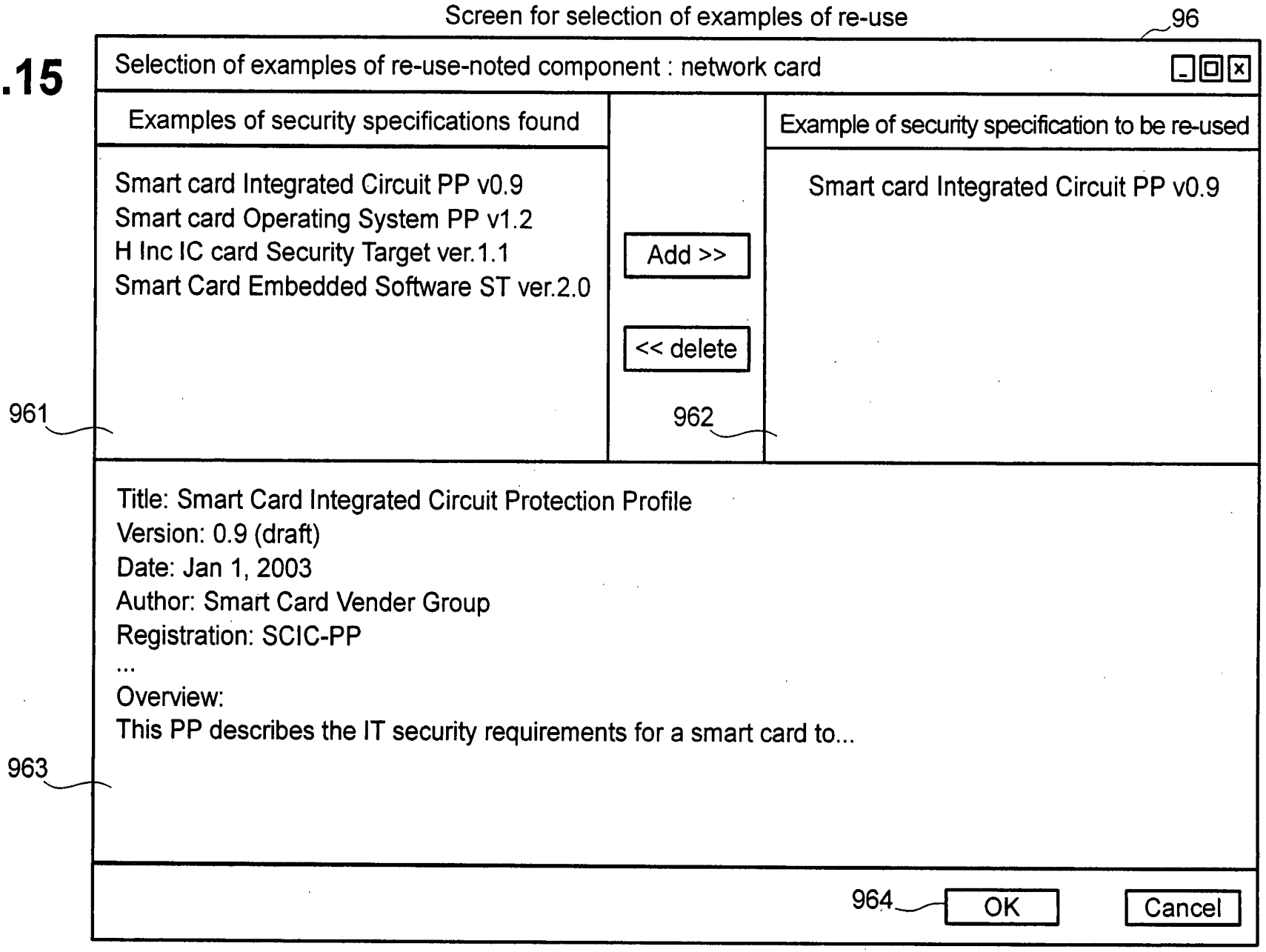
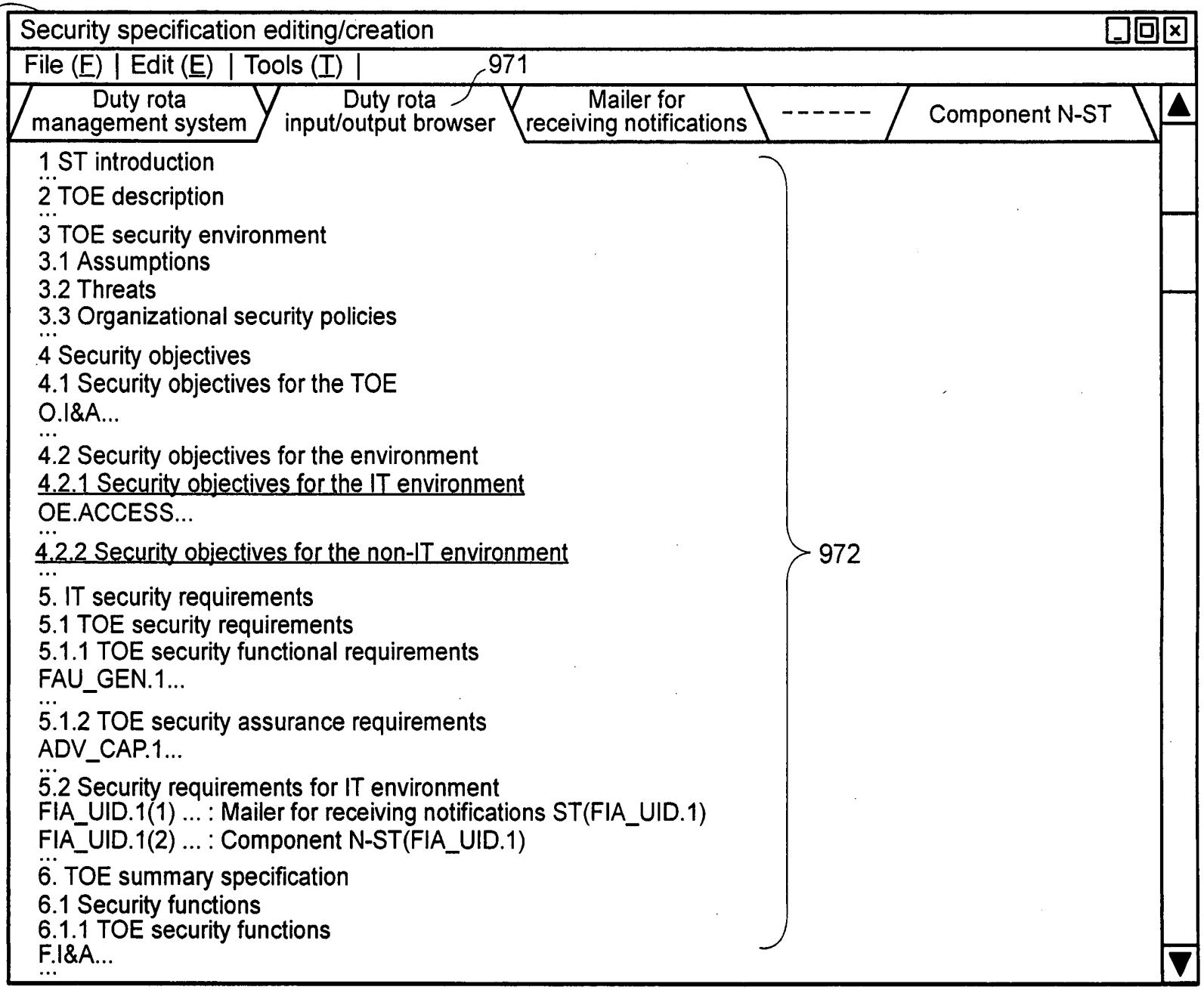
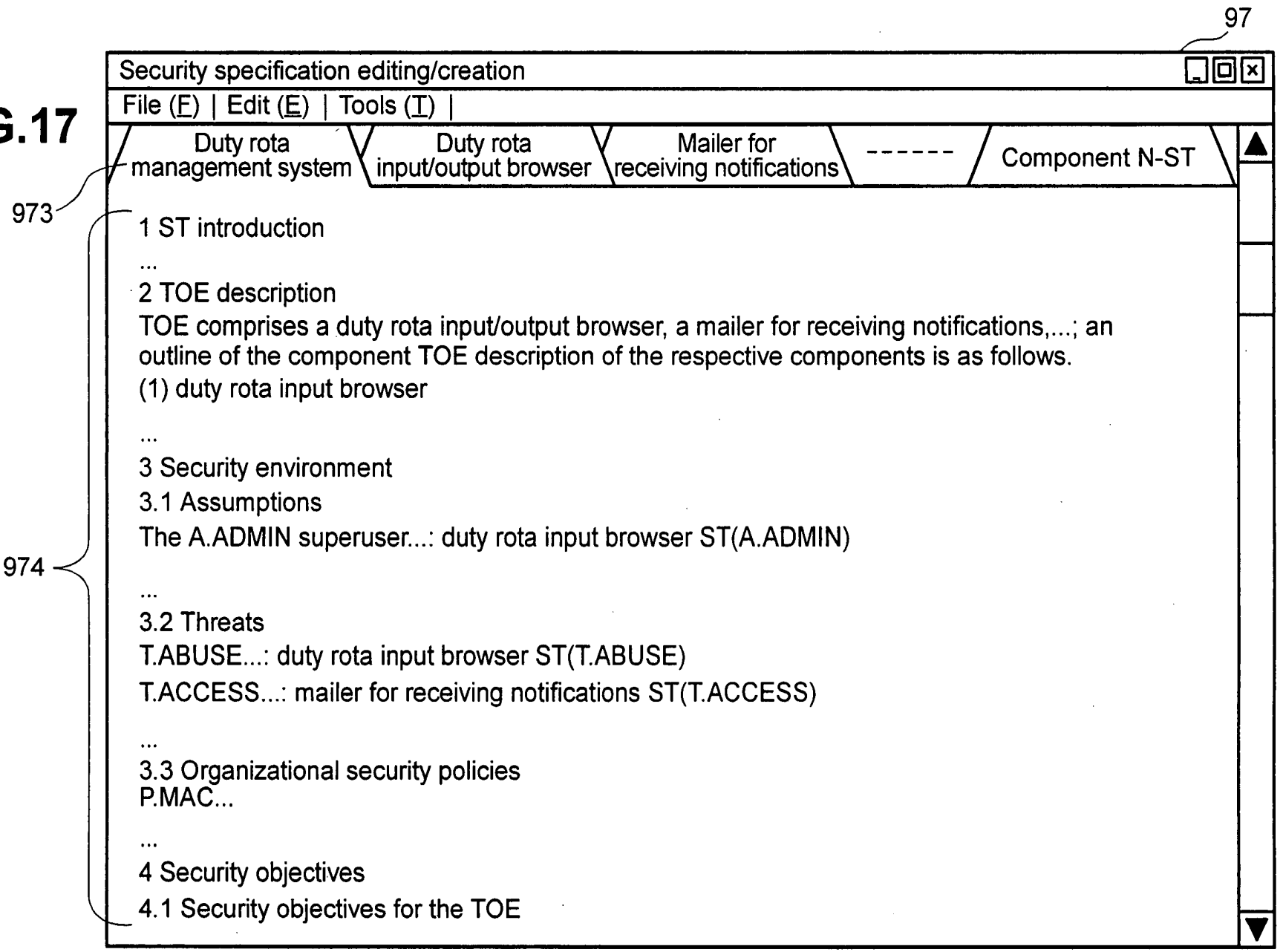

Screen for selection of examples of re-use
96
Selection of examples of re-use-noted component : network card
Examples of security specifications found
Smart card Integrated Circuit PP v0.9
Smart card Operating System PP v1.2
H Inc IC card Security Target ver.1.1
Smart Card Embedded Software ST ver.2.0
Add >>
<< delete
Example of security specification to be re-used
Smart card Integrated Circuit PP v0.9
961
962
Title: Smart Card Integrated Circuit Protection Profile
Version: 0.9 (draft)
Date: Jan 1, 2003
Author: Smart Card Vender Group
Registration: SCIC-PP
...
Overview:
This PP describes the IT security requirements for a smart card to...
963
964
OK
Cancel

FIG.16


97
Security specification editing/creation
File (F) | Edit (E) | Tools (T) |
971
Duty rota management system
Duty rota input/output browser
Mailer for receiving notifications

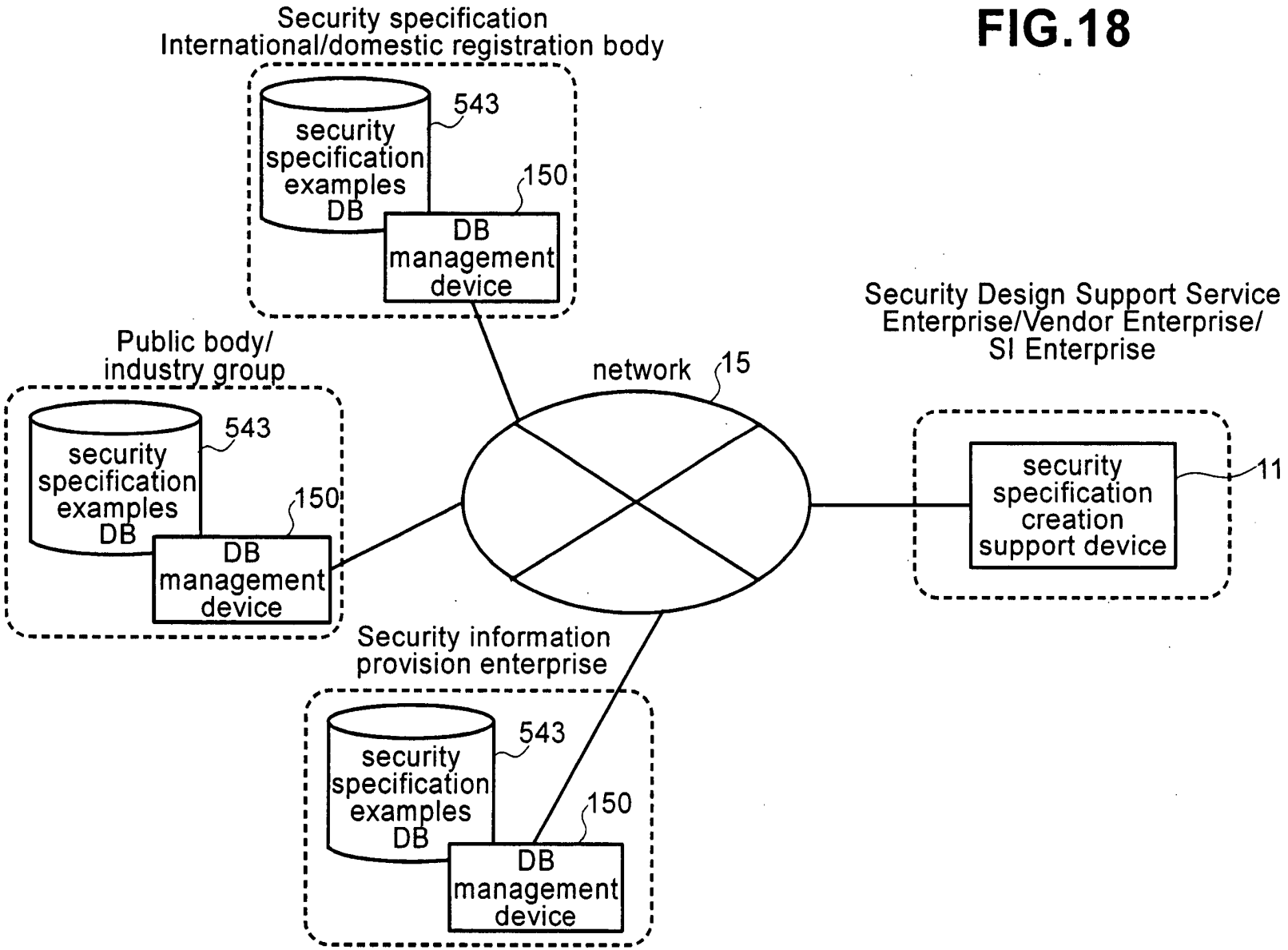
Component N-ST
1 ST introduction
...
2 TOE description
...
3 TOE security environment
3.1 Assumptions
3.2 Threats
3.3 Organizational security policies
...
4 Security objectives
4.1 Security objectives for the TOE
O.I&A...
...
4.2 Security objectives for the environment
4.2.1 Security objectives for the IT environment
OE.ACCESS...
...
4.2.2 Security objectives for the non-IT environment
...
5. IT security requirements
5.1 TOE security requirements
5.1.1 TOE security functional requirements
FAU_GEN.1...
...
5.1.2 TOE security assurance requirements
ADV_CAP.1...
...
5.2 Security requirements for IT environment
FIA_UID.1(1) ... : Mailer for receiving notifications ST(FIA_UID.1)
FIA_UID.1(2) ... : Component N-ST(FIA_UID.1)
...
6. TOE summary specification
6.1 Security functions
6.1.1 TOE security functions
F.I&A...
...
972

FIG.17


97
Security specification editing/creation
File (F) | Edit (E) | Tools (T) |
Duty rota management system
Duty rota input/output browser
Mailer for receiving notifications

Component N-ST
973
974
1 ST introduction
...
2 TOE description
TOE comprises a duty rota input/output browser, a mailer for receiving notifications,...; an outline of the component TOE description of the respective components is as follows.
(1) duty rota input browser
...
3 Security environment
3.1 Assumptions
The A.ADMIN superuser...: duty rota input browser ST(A.ADMIN)
...
3.2 Threats
T.ABUSE...: duty rota input browser ST(T.ABUSE)
T.ACCESS...: mailer for receiving notifications ST(T.ACCESS)
...
3.3 Organizational security policies
P.MAC...
...
4 Security objectives
4.1 Security objectives for the TOE

FIG.18


Security specification
International/domestic registration body
543
security specification examples DB
150
DB management device
Public body/
industry group
543
security specification examples DB
150
DB management device
network
15
Security Design Support Service
Enterprise/Vendor Enterprise/
SI Enterprise
security specification creation support device
11
Security information
provision enterprise
543
security specification examples DB
150
DB management device